WHAT IS CLAIMED IS:

1. A graphical user interface for an intrusion detection system, the graphical user interface comprising:

a field that depicts a summary of anomalies identified as part of a event that is detected in a network, the summary indicating event severity details of the event; and

an alert action region including a control to permit a user to snooze future alerts related to the event in the summary for a period of time.

2. The graphical user interface of claim 1 wherein the snooze control feature can be selected based on event types and roles of hosts.

3. The graphical user interface of claim 1 further comprising:

a control to allow a user to clear an alert if the alert appears on the overview page.

4. The graphical user interface of claim 3 wherein an event details region of the graphical user interface depicts anomalies that were used to classify the event.

5. The graphical user interface of claim 1 wherein details of events include values of source, destination, and protocol that caused an event to be raised.

6. The graphical user interface of claim 1 wherein event severity is coded by an indicia.

7. The graphical user interface of claim 1 wherein the interface includes a control to clear a selected alert.

8. The graphical user interface of claim 1 wherein the interface includes a details control that allows a user to observe details about a selected anomaly.

9. The graphical user interface of claim 1 wherein the details control presents a list of IP addresses to which the host attempted to connect.

10. A method comprises:

providing an operator with a list of events identified by an intrusion detection system, within the list of events being information indicating event severity, with severity determined based on an event having a percentage relationship to an established threshold for issuing an event notification; and

displaying the details of a selected one of the events to a user a user can "snooze" future alerts related to the selected event.

11. The method of claim 10 the control allows an event to be snoozed for a fixed period of time.

12. The method of claim 10 wherein the snooze control can be for selected event types and roles.

13. The method of claim 10 further comprising:

clearing a selected alert from the list of events.

14. The method of claim 13 further comprising:

displaying event details including anomalies that were used to classify the event.

15. The method of claim 14 further comprising:

displaying event details that indicate normal operating conditions of a host and current operating conditions of a host to allow the operator to take an appropriate action.

16. The method of claim 15 wherein one of the operating conditions displayed is normal and current connection rates of the host.

17. The method of claim 15 wherein the type of events include "worm propagation, unauthorized access, denial of service attacks, and historical anomaly.

18. The method of claim 10 further comprising:

displaying event details including destination and source fields populated with IP addresses and role classification of the host in the network.

19. The method of claim 10 further comprising:

displaying actions taken by the operator for the particular event.

20. The method of claim 10 further comprising:

displaying network statistics; and

displaying a ranking of hosts in the network according to a network statistical measure.

21. The method of claim 10 wherein the network statistical measure is a number of bytes per second and packets per second of each type of protocol observed in the system.

22. A computer program product residing on a computer readable medium for producing a graphical user interface for an intrusion detection system, the computer program product comprising instructions for causing a computer to:

render a graphical user interface on an output device, the graphical user interface comprising:

a field that depicts a summary of anomalies identified as part of a event that is detected in a network, the summary indicating event severity details of the event;

an alert action region including a control to permit a user to snooze future alerts related to the event in the summary for a period of time.

23. The computer program product of claim 22 wherein the snooze control feature can be selected based on event types and roles of hosts.

24. The graphical user interface of claim 22 further comprising instructions to render in the graphical user interface:

a control to allow a user to clear an alert if the alert appears on the overview page.

25. The computer program product of claim 22 wherein an event details region of the graphical user interface depicts anomalies that were used to classify the event.